Journal of Military Ethics

Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/smil20

The ethics of espionage
Tony Pfaff & Jeffrey R. Tiel

a 7816 Welch Ct, Alexandria, VA, 22315, USA Phone: +1 703 697 2239 E-mail:
b Ashland University, Ashland, OH, 44805, USA Phone: +1 419 289 5154 E-mail:
P Published online: 15 Aug 2006.

To cite this article: Tony Pfaff & Jeffrey R. Tiel (2004): The ethics of espionage, Journal of Military Ethics, 3:1, 1-15
To link to this article: http://dx.doi.org/10.1080/15027570310004447

PLEASE SCROLL DOWN FOR ARTICLE

Full terms and conditions of use: http://www.tandfonline.com/page/terms-and-conditions

This article may be used for research, teaching, and private study purposes. Any substantial or systematic reproduction, redistribution, reselling, loan, sub-licensing, systematic supply, or distribution in any form to anyone is expressly forbidden.

The publisher does not give any warranty express or implied or make any representation that the contents will be complete or accurate or up to date. The accuracy of any instructions, formulae, and drug doses should be independently verified with primary sources. The publisher shall not be liable for any loss, actions, claims, proceedings, demand, or costs or damages whatsoever or howsoever caused arising directly or indirectly in connection with or arising out of the use of this material.
The Ethics of Espionage

Tony Pfaff

7816 Welch Ct, Alexandria, VA 22315, USA
Tel: +1 703 971 0421, E-mail: tpfaff@aol.com

Jeffrey R. Tiel

Ashland University, Ashland OH 44805, USA
Tel: +1 419 289 5154, E-mail: jtiel@ashland.edu

Professional soldiers and academics have spent considerable effort trying to conclude when it is permissible to set aside the usual moral prohibition against killing in order to achieve the goals set before them. What has received much less attention, however, is when it is appropriate to set aside other moral considerations such as the prohibition against deception, theft and blackmail. This makes some sense, since if it is moral to kill someone, whether or not it is appropriate to deceive him seems to be trivial in comparison. But members of the intelligence community, both military and non-military, must determine for times of peace as well as war when it is appropriate to set aside the usual prohibitions in order to achieve national objectives. The purpose of this article is to provide a framework for military and non-military intelligence professionals for answering and discussing these questions. By applying insights from Kantian and Lockean ethics, the authors seek to describe an ethic of the intelligence profession that permits a combination of ethical restraint and intelligence effectiveness.

KEYWORDS: military ethics, intelligence ethics, Kant, Locke.

Effective espionage requires intelligence officers to deceive, incite, and coerce in ways not acceptable for members of the general public. And the public these officers serve has on occasion objected morally to some of the activities conducted in their name. The fact that intelligence agencies often have trouble obtaining permission to recruit on college campuses because of moral objections to the profession serves to underscore this point. Further, intelligence officers themselves are just as concerned about the moral nature of the profession. According to a 1998 study, many members of the CIA expressed concern that serving a perceived ‘cloudy moral purpose’ made it more likely that people will become corrupted by the ‘dirty’ aspects of the profession (Pekel 1998: 88–89).
However, the temptation to ignore such moral considerations can be intense. The events of 11 September only serve to highlight this point. Many blame the ability of the hijackers to carry out their plan relatively unimpeded on failures within the intelligence community to provide timely information that would have allowed law enforcement agencies to intervene. With the possibility of such events in the future, intelligence professionals feel considerable moral pressure to accomplish their missions. This means that taking into account ethical considerations that seem to undermine an intelligence officer’s effectiveness will not always be morally compelling.

In fact, in the wake of 11 September, there is much talk that it is now time to ‘take the gloves off’. There is concern, however, that in taking the gloves off, intelligence agencies may go too far and betray the trust the public places in them. But any discussion of proper intelligence operations during wartime requires an understanding of the justification and moral limits of intelligence operations in peacetime. In this essay we will attempt first to offer a general justification for effective espionage, a justification which can extend to all the various aspects of the world of intelligence, including human intelligence gathering, signals intelligence gathering, photoreconnaissance intelligence gathering, all the various kinds of analysis and reporting to the policy makers, as well as the covert operations elements. Second, we will apply the general theory to just the specific case of foreign human intelligence gathering in peacetime, leaving aside more extreme measures like physical coercion that might be permissible, though still controversial, during wartime intelligence gathering, as well as the full gamut of non-intelligence gathering espionage activity.

We should add one caveat as a general condition on this paper. We are attempting to offer what might be called a formal moral theory that permits an evaluation of the conduct of rival intelligence agencies without a complete evaluation of the substantive moral standing of the regimes that they serve. We think this a valuable project, since theories resting significantly on the ethical standing of the regime make it all too easy for intelligence officers on either side to delude themselves into thinking that they are on the side permitted the ‘special’ courses of action open only to those fighting the ‘bad guys’. Moreover, once one side (perhaps rightly) elects to operate in this ‘special’ manner, inevitably the other side will reciprocate. Thus, it is helpful to provide a common guide of conduct for the profession of the intelligence officer, regardless of the substantive nature of his regime.

Drawing the Line: The Moral Boundaries of Foreign Intelligence Gathering

That all persons are created equal is the central tenet of the underlying political philosophy that grounds modern liberal republics. This fact suggests that the agencies that defend these regimes must recognize this as a constraint on the kinds of actions they may pursue. To do otherwise would be an act of betrayal. Furthermore, since this foundational belief is meant to encompass all people, this constraint extends to all persons, and not just to those they have sworn to defend.
This is not to say that members of the intelligence communities have the same obligations to citizens of other nations as they do to citizens of their own, but it does mean that there is a certain level of respect they owe to citizens of other nations that should constrain their actions to some degree.

But to say that all people have equal value is not to place any meaningful constraints on the kinds of actions one may commit. One could treat others equally badly or equally well depending upon what one believes about the moral status of the individual in the first place. If human life deserves no special respect, then there are no moral reasons to constrain the kinds of acts that affect those lives. The idea that human life is somehow fundamentally valuable and deserves a special respect is, of course, not new, nor particularly controversial. It is the second central commitment of our contemporary liberal republics, as well as a key feature in the teachings of many of the world’s religions and moral philosophies.

While theories of human nature compete over how to locate the cause of human dignity, certain salient features appear critical to human value. The first is metaphysical freedom. Unlike rocks, human beings have the capacity to reflect upon and decide their actions. To use Kantian language, human beings can respond to reasons as well as to causes. The second feature is rationality, or the capacity to recognize universal commonalities among objects and identify oneself as a person possessing such commonalities. Hence, we can not only recognize our own freedom for choosing, we can recognize that feature in common with the other persons we call human beings.

This natural equality (of freedom and rationality) entails the principle of universalization, that whatever holds good for me in virtue of my free rationality holds good for you in virtue of yours. Hence, I should not treat you in a way that would be incompatible with the way that I need to be treated for upholding my own freedom and rationality. This principle has been captured to varying degrees by the Golden Rule—that one ought to treat others as he himself would like to be treated, by Locke’s Natural Rights—that one ought to respect another’s life, liberty, and property just as one expects another to respect his, and Kant’s Categorical Imperative.

Drawing from Locke and Kant, we can further argue that as equally free rational agents, human beings possess the freedom or liberty to do what they will, provided they stay within these fundamental moral boundaries unless they consent to be constrained by something in addition to these boundaries. This principle yields two important considerations. First, consent is a central moral criterion on evaluating our behavior toward others. Murders, thefts, and lies can all be recognized to be wrong, in part because they are violations of consent: no one consents to be murdered or to have his goods stolen. If he tried, we would not classify the resultant action as ‘theft’ at all. Consent plays such a critical role in moral reasoning, because it is the manifestation of the freedom of the person. Kant recognized this in one of his formulations of his famous Categorical Imperative:

Act in such a way that you always treat humanity, whether in your own person or in the person of another, never simply as a means, but always at the same time as an end (Kant [1785] 1964: 96).
Failure to abide by someone else’s consent causes me to treat that person as a non-person, more like a tool than a user, merely as a means to my ends, not as a self-determining agent capable of choosing his own ends. In Kantian terms, treating someone as a self-determining agent, or an ‘end’, is synonymous with respecting the dignity of that person’s freedom. Treating others as an end and not merely a means requires one to adopt a stance towards fellow human beings that demands moral impartiality. It requires that we recognize the limits another’s refusal to consent entails for our conduct.

We can now turn to the second consequence of the principle that as equally free rational agents, human beings possess the freedom or liberty to do what they will, provided they stay within the fundamental moral boundaries unless they consent to be constrained by something in addition to these boundaries. Just as consent restrains what human beings may do to one another, so it also enables what they may do to one another. Through consent, human beings may enter into one of the most profound forms of limited liberty, citizenship, a relationship between persons that authorizes the powers of government for the preservation of the fundamental moral rights discussed earlier. Since governments exist for this purpose, they acquire the derivative right of collective self-defense, just as individual free agents possess the rights of individual self-defense and third-party defense.¹

But with the expectation of governmental protection come the duties usually associated with that protection including participation in governing, financial support through taxation, and physical support in emergency and military crises. Since people decide whether or not they will act as citizens of their respective countries, in effect choosing to be citizens, they can be held responsible for that choice. That responsibility will prove most instructive as we shortly discuss not only the limits but the moral permissibilities in intelligence-gathering.

As citizens have responsibilities to their respective governments (articulated in their traditions, laws, and constitutional orders), governments likewise have duties to their citizens, one of which is a duty to be prepared to defend the rights of their citizens. This duty includes an expectation that other nations or foreign groups may attempt to violate these rights, just as this duty includes an expectation that individuals within one’s country may attempt to violate the laws. Preparation for rights-enforcement includes enforcement preparedness (in both military and police contexts) and intelligence gathering (in both foreign and domestic contexts). Therefore, governments have a duty to determine what threats lie on the horizons for their citizens, a duty which offers a moral justification—even stronger—a moral requirement for intelligence-gathering.² To fail to engage in intelligence-gathering would be to shirk a moral duty lying at the core of a government’s responsibility, for without timely information as to a potential enemy’s capability and intentions, civic defense is impossible.

¹ We are assuming that the readers are familiar with the usual arguments deriving the rights of self-defense and the authorization of lethal force from the right of the preservation of life. It is our view that admitting individual self-defense and individual third-party defense authorizations together with the principle of derived powers for governmental authority entails the legitimacy of governmental use of lethal force in military contexts.

² This moral necessity has been recognized in the Hague Convention (Wells 1996: 434).
To make this clearer, we might borrow an analogy from Lieutenant Colonel Mark Mattox in his essay, ‘The Moral Limits of Military Deception’. Mattox offers the example of a football game and the shared expectations that result from those engaged in the playing of the game. These ‘shared expectations’ are the rules of the game consented to by both the players and the spectators of the game, though in importantly different ways. Consonant with the rules, both teams may attempt to deceive each other even though this is clearly using the other as a means. But since nothing interferes with their choice to play the game, they are also being respected as ends (i.e., not used merely as means). In this context, the fact that one team is completely overwhelmed by some deception is not the fault of the deceiving team, but of the deceived team for failing to play well by discerning and counteracting the other team’s strategy (Mattox 2002: 9–12).

Failure to abide by the rules of the game, however, will result in the end of the game itself. Hence, certain kinds of conduct in the game are impermissible, conduct that contradicts the conditions on the game’s being played. But it is conduct that undermines the playing of the game for both sides, akin to the golden rule ethical principles articulated earlier. Any kind of conduct that results in such self-defeat, in the de facto cessation of the game, is irrational relative to the game. Any kind of conduct in intelligence-gathering that results in self-defeat, in the de facto cessation of respect for the other party’s (and derivatively, my side’s) free agency, is likewise irrational relative to the ethics of intelligence.

But, since espionage is enabled by the consent of individual citizens seeking the protection of their governments, actions may be taken against them with respect to intelligence-gathering, because they have joined ‘the game’. Some people join the game as spectators, while others join the game as players, but joining is something that everyone does insofar as he is a citizen at all. In what follows we will discuss the different kinds of conduct that may be employed against the players versus the spectators in the world of espionage.

We should add that the ethics of intelligence concerns not only who is targeted as a potential source, but also the kind of information sought. What gives a nation a right to possess information the other side regards as secret is that if it did not possess it, its national security would be severely compromised and its citizens would be placed at great risk. Conversely, this means that it would be wrong to conduct intelligence operations to obtain secrets that do not enhance national security. Let us imagine a case where it was permissible to use a listening device in someone’s bedroom to determine whether that person was a potential source. After enough surveillance was conducted to determine that the person in question had no information relevant to our side’s national security, it would be morally impermissible for us to leave the bug in the bedroom because the person’s sex life was particularly entertaining.

Legitimate Targets of Espionage

While the role of the soldier is to deter or defeat threats, intelligence professionals must find and assess those threats in the first place. Thus, they must cast a wide net sometimes directed at people and nations who do not and never will represent any
kind of threat. As philosopher Thomas Nagel notes, it is not fair to target just anyone in war: there must be ‘something about that person’ that justifies it. A person in an enemy state who accepts the training and equipment of a soldier and then takes to the field of battle becomes such a threat, and may be killed. But once he ceases to be a threat, whether through surrender or incapacitating injury, it is no longer permissible to harm him. For these reasons, Nagel argues, it is also never permissible to target directly his family or personal property since that is not what makes him a threat (2000: 210).

This same principle will hold true in the world of intelligence-gathering. In this case, however, the feature that will make persons subject to espionage operations is that they possess or are likely to possess secrets that threaten national security. Thus, just as it is not ‘fair’ to tackle a spectator in football (even though he is rooting for the opposing team,) it is not justifiable to conduct certain kinds of intelligence operations against non-players, even if they are citizens of unfriendly or even threatening nations.

But unlike the case of the soldier who can be readily identified by his uniformed status, potential sources of information will likely be concealed among the camouflage of ordinary civilian life. Thus, preliminary intelligence gathering must be permissible against persons who may turn out to be wholly innocent of possessing any vital information. Just as a hacker might send a program to examine thousands of computers for vulnerability, so intelligence agencies must possess a means to determine who are the likely sources of critical information beyond the obvious candidates like foreign military personnel, foreign intelligence officers, foreign government personnel, etc. In this section we will examine kinds of legitimate targets consonant with the following principle: the degree of consent to participate in the world of national secrecy on all levels of a country’s self-defense structures together with the quality of information possessed proportionately permit increasingly invasive means of attempting to acquire that information by foreign powers. Thus, there is a direct link between the legitimacy of the kind of target and the legitimacy of the means employed against him. In this section we will discuss five categories of intelligence targets and five degrees of invasiveness in intelligence collection that we think are morally permitted consonant with the ethical principles outlined earlier. In the next section we will offer detailed moral justification for the invasive manner of intelligence collection.

The first kind of intelligence target is the ordinary citizen. This might seem surprising, since the game analogy offered earlier might have suggested that only those playing the intelligence game can be legitimate targets of an intelligence operation. But this would be an erroneous inference, for in the world of citizenship everyone is a player, though not to the same degree. By functioning as citizens of a foreign power, the average citizen renders himself vulnerable to those elements of intelligence-gathering necessary to fulfil the goal of preliminary intelligence gathering: identifying the real sources of information.

The second kind of intelligence target is the person discovered to be aware of critical information but unaware of its value or his value in the world of defense-secrecy. We believe this kind of person to be rare, since governments tend to treat people possessing these kinds of knowledge differently than other citizens (background checks, polygraph tests, odd interviews, classification of data desired for publication, etc.).
In both the first and second cases, the persons are legitimate targets of intelligence-gathering, though neither has consented to 'play the game' beyond his status as a citizen. Hence, the kinds of activities that may be employed against them are proportionately greater in limitation. Some examples might be helpful.

Imagine a person working at a chemical laboratory with corporate ties to a company whose other holdings include companies that conduct defense research. It might be the case that the chemical company also conducts defense research, but is using the 'chemical company' name as a cover for its real purpose. It would be perfectly permissible to target the employees of this company for intelligence gathering purposes in the preliminary way to see whether they are sources of valuable information or not. Once it was deemed that they were not such sources, it would be ethically required that the intelligence operation against them cease, although periodic reviews would be permissible.

Imagine a person in the second category working for the defense research arm of the same corporate headquarters referred to earlier but in a company with a cover as a candy manufacturer. Suppose that the person worked at the candy company as an elevator maintenance worker and had no idea that the company actually conducted defense research. His use as an intelligence source would be his knowledge of the elevators were they ever to be necessary for use in an operation to break into the facility to acquire the technology, though he himself was blissfully unaware of his importance. An operation directed against this person to acquire information about the elevators would be permissible so long as it involved no coercion against him.

In neither of these cases is one required to restrict one’s intelligence-gathering solely to public sources. On either of these levels, deception would be permissible as part of the intelligence-gathering operation. But one would not be permitted to employ more invasive forms of intelligence gathering that we shall shortly see legitimated by the adoption of a more significant 'player' status.

The third category of legitimate targets of intelligence gathering is someone discovered to be aware of critical information and aware of its value or his value in the world of defense-secrecy, but not (yet) aware that you are targeting him as a source. Imagine the case of a spouse of a defense worker whom we realize is having conversations with her husband that involve classified information. Her choice to very obviously violate her own country's secrecy laws and inquire after her husband's occupation, and her husband's foolishness in revealing elements of his work to her, are two acts of consent that put her into the 'game' much more than either of the former categories. Both she and her husband are legitimate targets of intelligence gathering of a fairly invasive kind, including the possibility of gathering information useful for blackmail should they discover that they are being used as sources. In other words, information may be gleaned that involves not only their knowledge in the game itself, but involves keeping them as players in the game. Thus, deception, incentives for recruitment, and potentially blackmail for deeds they have actually committed may be used against them. So, if we discover that the wife is having an affair with another man, as a legitimate target in the third category we may permissibly threaten to reveal this to her husband. Notice that her own choices have put her into this situation, namely trying to determine information about her husband’s profession and having the affair. And her own choices can remove her from the situation: confessing to her husband both her affair and the fact that she’s
been approached for recruitment (something that they would both have to immediately report to their authorities). It would be impermissible to manufacture evidence to blackmail or extort her, since this exceeds the degree to which she has consented to participate in the intelligence-world, and since as a non-intelligence-professional, she could be subject to sanction for which there is little chance she could be cleared. She would be being used merely as a means to our ends, rather than as a means to ends she by her own conduct has sanctioned.

The fourth category of legitimate targets of intelligence gathering is someone discovered to be aware of critical information and aware of its value or his value in the world of defense-secrecy, and happily aware that you are targeting him as a source, because he is disposed toward releasing the information to you. This is the case of a potential intelligence officer, someone who for whatever reason (whether noble or not) is consenting to reveal information to you. This case might seem to be the least problematic, because it involves the consent of the key party. But it does involve some very complicated moral problems, because the person in question is apparently morally obligated under his citizenship commitments not to commit treason against his country. Unlike the case of the blackmailed wife, her being blackmailed functions morally to mitigate against her conduct as being fully treasonous (at least morally, if not legally). But in our fourth case the conduct is clearly and fully treasonous, and how can a nation encourage behavior in foreign citizens that is flatly immoral?

The answer lies in recognizing the full import of what occurs when a person becomes an intelligence officer: in effect, it is a transfer of citizenship. This is clear from the fact that intelligence officers often desire the protection of their case-officers and their intelligence agencies: they demand that the civic-protection role formerly played by the old regime be replaced by the new one. As citizens of a new country, intelligence officers shed their duties toward their old regimes, but acquire clear duties to their new ones. Similarly, the new country has duties towards its new agent-citizen including not disclosing that the person is an agent. According to R.V. Jones, an intelligence professional in World War II and noted scholar in the field, there were allegations that Allied intelligence professionals considered betraying a German double agent by letting another agent 'sell him out'. By betraying that agent, the other agent would ingratiate himself to the Germans and be in a position to pass false information regarding the landings on D-Day (Jones 1989: 43). According to Jones, this did not happen and would have been viewed by the intelligence community at the time as unacceptable. There are obvious practical downsides to such a practice, since it will be hard to recruit agents if they believed you would likely betray them, and it will be hard to trust information received from one’s agents if they think that they might be betrayed. But there are ethical

---

3 We are leaving aside the duty that a citizen may have to declare a change of citizenship publicly. We are divided about whether such a duty exists, and its consequences. This may be a case in which the moral nature of the regime impacts the duty of disclosure. In other words a person rejecting a tyrannical regime and offering to work as an agent for a just one may have no duty to reveal the changed status, while someone in the reverse may well be committing treason (morally as well as legally), because the host state did nothing violating its terms of the political compact.

4 Cases in which an agency recruits an agent under the pretense of being an alternative agency (e.g., Mossad might attempt to recruit an Arab informer by pretending to be the CIA) pose real difficulties for this citizenship theory of agent-handling.
problems with such practices as well, since they treat someone who has consented to place himself in your protection as the moral equivalent of a citizen (on our theory) as a mere means to an end.

The fifth category of legitimate targets of intelligence gathering is someone discovered to be aware of critical information and aware of its value or his value in the world of defense-secrecy, and an actual participant in the intelligence world as an intelligence professional. This person is subject to the most invasive forms of intelligence gathering, since he is most fully a ‘player’ in the game and by joining an intelligence agency has fully consented to its rigors. He may be deceived, incited to recruitment, or blackmailed over things that he has done, as well as blackmailed for reasons that are manufactured against him. Short of physically harming him in his home country (wartime cases would obviously differ here), real or manufactured information may be used against him for coercion in any way subject only to the principle of double effect, a principle likewise limiting all four prior categories.

The principle of double effect is well-known in the military ethical tradition for its usefulness in enabling a soldier to determine whether an act that could indirectly result in non-combatant casualties can be justified (Christopher 1994: 52). Similarly, intelligence operations directed against legitimate targets might have nonconsensual consequences for illegitimate targets. Cases of deception might be passed on toward other persons who then believe a falsehood. Cases of blackmail might have long-term consequences for other persons involved in the blackmail case or an innocent family member who might be harmed via association if certain information were exposed. The doctrine of double effect offers a means to sort through our obligations to illegitimate targets of espionage and determine how those obligations impact what is permissible in our operations against legitimate targets.

Advocates of the doctrine of double effect recognize a moral difference between the consequences of our actions that we intend and those we do not intend, but still foresee. Thus, according to this doctrine, it is permissible to perform a good act that has bad consequences, if certain other conditions hold. Those conditions are: (1) the bad effect is unintended, (2) the bad effect is proportional to the good effect’s worth, (3) the bad effect is not a direct means to the good effect and (4) actions are taken to minimize the foreseeable bad effects, even if it means accepting an increased risk (ibid.: 93).

Double effect is much easier to understand when applied to real-world examples, so let us return to our female source in category three who possesses vital information and who is having an affair. Our threatening to release to her husband the information on her affair would be legitimate, because he himself is a legitimate target. But would it be legitimate to leak it to the local newspapers? Let us add to the story an additional condition: a child. Wouldn’t the child’s life be harmed if the story were leaked to the newspapers and a prominent family was exposed in an adulterous affair? If so, then a person against whom the operation is not intended would be harmed by the action of blackmail, and we must use double effect to determine whether the blackmail is permissible.

---

5 This doctrine was developed in response to Augustine’s prohibition against self-defense. Augustine held that self-defense was inherently selfish and that acts motivated by selfishness were not morally justifiable since selfishness is not morally justifiable.
The first condition requires the child’s harm be unintended. We can stipulate this for purposes of this scenario. Harming the child furthers no unrelated national security objective. The second condition requires that the child’s harm be proportional to the desired intelligence objective. Is the possibility of public embarrassment to a child worth the value of maintaining this woman as a source? Several considerations are in order here. First, the choice to reveal the information is partly hers in virtue of her choice to have the affair in the first place, and the information on the affair may have arisen in the public domain in its own time in any case. But we would have to actually reveal the information in this case and so we would be responsible, regardless of what might happen if we did not act. Second, if we grant that the information in question is valuable enough, then the public exposure of the child is worth it. Third, it is worth noting that the woman’s refusal to function as a source may well mitigate against our revealing the information anyway, since her value to us is blown and our revealing her situation may risk our own exposure. So, at best we might realistically only threaten her with public exposure.

The third condition requires that the child’s embarrassment not function as a direct means to the blackmail of the source, and here things become very complicated morally. Obviously, the child’s embarrassment might function on the psyche of the mother to extort her continued cooperation. But if this were the ‘direct means’ of blackmail, then it would violate double effect and render the operation immoral. It is possible, however, that we did not intend this as part of the blackmail at all, but once we discovered the effect of the blackmail, we might find it very difficult not to count on it in our calculations. Thus, this third condition would force us not to go public with the information on the affair, but only to reveal it to the husband, or threaten to reveal it publicly with the knowledge that we could not morally carry out the threat. Under double effect it is sometimes permissible to threaten to do something that would be immoral (not in itself, but due to the proportionality condition) to actually carry out.

One of the harsh realities of modern war, and one may argue, a modern intelligence operation, is that people who are not directly involved nonetheless do not have a reasonable expectation not to be harmed by it. They do, though, have a reasonable expectation that they will bear significantly less risk than those involved. They also reasonably expect that both sides will minimize the occasions and effects of this harm even if that means changing the nature and goals of specific operations in order to do so. Thus, while intelligence professionals are permitted to engage in deception and blackmail in order to fulfill their roles, they must take great care when these activities involve innocent people, people who have no reason to expect to be targets or subjects of such activities. Thus when such operations involve innocents, they should be avoided and other means of gaining this information should be pursued. If this is not possible, and the information is vital, then limitations imposed by the doctrine of double effect must be observed.

The Morality of Deceit, Incitement, Bribery, Blackmail, and Appropriation

We have detailed a number of kinds of activities that we have broadly claimed are morally permissible in the ethics of intelligence-gathering, so long as they are
directed against the proper kinds of targets in accordance with the five levels of those targets’ consent. In this final section, we will explain how the moral importance of consent justifies the use of deceit, incitement, blackmail, and appropriation in intelligence-gathering.

It might be useful to stipulate a preliminary set of distinctions to avoid confusion later. We will employ the terms ‘lie’, ‘steal’, ‘adultery’, and ‘murder’ as moral violation terms \textit{per se}. We will treat moral violations as unexceptionable and their permissible equivalents as non-moral actions. So, murder is always wrong (moral term), while killing is not (non-moral term). Adultery is always wrong (moral term), while sex is not always wrong (non-moral term). Theft or stealing is always wrong (moral terms), while appropriation is not always wrong (non-moral term). Lying is always wrong (moral term), while deliberate falsehood or deception is not always wrong (non-moral terms). Ethicists of war and intelligence do themselves a service by avoiding the impression that they really think that it is permissible to murder people in wartime. Admitting this makes it very difficult to identify atrocities as the murders that they really are. Similarly, many people are seriously confused by questions of whether it is morally permissible to lie to the Nazis when they come asking about the Jews, when deceiving Nazis is perfectly acceptable and not lying at all. ‘Murder’ and ‘lying’ carry with them morally disapprobative force, and therefore we think it prudent to avoid confusions in their employment.

Deception

On occasion, intelligence professionals must create a cover identity for themselves or for some other agent in order to gain access to information they could not get any other way. Additionally, creating this cover story may involve falsifying academic and professional records and credentials. In such cases it seems they are using the people who will hire or place them based on those credentials simply as a means to an end. Furthermore, it may require them to deceive their own family, friends, and employers about what they really do. Is this kind of deception morally permissible? It is interesting to note that Kant saw deception as inherently wrong because it diminished a person’s capacity for acting morally (Kant [1797] 1963: 140–141). Acting morally requires the ability to act rationally. Acting rationally requires acting on the best information available relevant to a particular moral problem. If one intentionally provides another with false information, then one has made it difficult, unless the truth is uncovered, for that person to act morally. For this reason, most kinds of deception are going to be wrong because deception is incompatible with respecting the inherent value and dignity of human beings.

But this does not require that we accept all forms of deception as immoral (Mattox 2002: 5–7). Just as the quarterback may deceive the opposing team as to what the next play is or take the ball from them, intelligence professionals are free to engage in at least some kinds of deception against anyone who is a legitimate target. This is not cheating because the other ‘team’ is supposed to expect it, and in virtue of our consent doctrine, has consented to intelligence gathering and the necessity of deception for its furtherance.
An analogy in domestic life might prove useful: we purchase theater tickets and expect to be deceived about the details of the actor’s life on the stage. If he really told us his own story, we would be outraged, because we are ‘buying a lie’. But of course, it is not a ‘lie’ at all, but a deliberate falsehood to which we have consented. Participation in the self-defense apparatus of a government and even minimally in citizenship is an explicit form of consent to deception on multiple levels, since one expects one’s own government not to reveal its own secrets even to its own people. The people’s ‘right to know’ is a myth confused with the legitimate right of the people to accountability. The latter does not require a general unveiling of all secrets.

Since secrets are explicitly granted authorization in one’s own government, it follows via universalization that they are likewise granted in the governments of foreign nations. And with secrecy arises the potential of harm and the authorization for espionage to ferret out information about that potential harm. Both sides in this determination to discover each other’s secrets authorize their own side to employ deception and, therefore, both sides grant the other side the same authority. Hence, deception with respect to ferreting out that harm is justified.

But in much intelligence gathering activity there are those who may not be the direct targets of deception, but who are subject to it anyway, such as family, friends, and employers. These people are innocent of the kinds of activities that would otherwise make them legitimate targets and involving them would be self-defeating. Relationships with family members, friends, and employers rely on a great deal of trust. Deceptions, however, undermine this kind of trust and thus cannot be part of the shared expectations of people who have such relationships. Deceiving them is not permissible and thus should usually be avoided.

Sometimes, however, deceptions against people who have not ‘entered the game’ beyond the first level may be necessary to gather critical information or to prevent the disclosure of critical information. A husband of an intelligence officer may not know that his wife is an officer, and she may legitimately be ordered to deceive him about her role, a deception authorized by their mutual citizenship in the ordering country. Alternatively, a case officer may be walking to a drop site to retrieve some film only to be stopped and questioned by a local police officer. The case officer will undoubtedly omit any references to his intelligence gathering activities and simply recite his probable diplomatic credentials together with the diplomatic cover he maintains, and he may invent a perfectly plausible story for why he is on that street at that hour. All of this involves deceiving someone who under normal circumstances has some rights to expect truthful answers and who is not really beyond the first level in intelligence gathering. So, how can deceiving the police officer be justified? The answer lies again in the full ramifications of citizenship commitments: an explicit (or implicit, if it has not been thought through adequately) authorization toward deception for both sides’ intelligence officers was made when the police officer’s citizenship committed him to supporting his own government’s espionage activities. And our differing reactions to deception illustrate this. If I deceive a police officer and am discovered, my community will disapprove my deed. But if I am discovered, and it turns out that I am a friendly spy, the reaction will differ: ‘Oh, he only deceived the police officer because of his undercover role’.
Incitement, Bribery, and Blackmail

Incitement to reveal information is the next activity requiring moral justification in the world of espionage. Intelligence professionals actively recruit sources to provide them with information. Sometimes such foreign nationals do so willingly. Sometimes intelligence professionals offer an incentive such as money to induce cooperation. Sometimes they coerce foreign nationals into cooperating by means of blackmail.

It is not a problem to offer an incentive to a foreign national to become a controlled source. It does not matter if the foreign national does it because he loves our country, hates his, or just likes money—he is willingly engaging in this activity. Thus he bears the risks that come with it. What is much more problematic is when an intelligence officer blackmails a foreign national into providing information. But though it is problematic, it is not necessarily impermissible. If the individual committed the act for which he is being blackmailed, then he bears the moral responsibility for putting his state’s secrets at risk. If one possesses a secret, then one is obligated to protect it, which includes keeping oneself free of the risk of blackmail. Thus, just as the football team is free to exploit the weaknesses of the quarterback, the professional intelligence officer is free to exploit the weaknesses of certain foreign nationals—specifically those who constitute legitimate targets of intelligence operations—who possess secrets that pose a threat to national security. In such cases, it is important to remember that the foreign national can always refuse to give in to the blackmail and therefore his capacity for consent is preserved.

This does not mean, however, that there are not limits to the kinds of coercion in which spies may engage. A spy crosses the line (in all but the fifth level of legitimate targets) when he makes it impossible for the individual he is recruiting to choose otherwise. This is what it means to treat him merely as a means. For example, entrapping someone by manufacturing a blackmailable offense, so that he faces the choice of revealing the alleged offense and consequently suffering a severe sanction, or of cooperating with the agent, crosses the line, because the coercion is not grounded in the actual choices of the recruitment target. Furthermore, this clearly rules out threatening to blackmail friends or family members in order to get cooperation. If these others did not freely enter the game, it is not reasonable to expect them to bear the risks of someone who does.

The only exception is the intelligence officer himself in our fifth level of legitimate targets. By having fully entered into the intelligence game, he is vulnerable even to manufactured evidence. His own side ought to be prepared for this level of manipulation of the facts, and so it is never the case that it is impossible for his side to discover a way to believe its own officer. As such, he cannot ever be placed in a position where no one will believe him in principle.

But conduct of this kind is inappropriate between nations that view themselves on friendlier terms. A US operation of this kind against a British target, or as a recent television program fictionally portrayed, an Australian operation of this kind against a US CIA analyst, undermines the very foundations of ‘alliance’ even if one heeds the American Founders’ counsel against becoming ‘friends’ with any foreign power. Thus, actions of this kind are permissible against hostile nations, ambiguous against neutrals, but clearly out of bounds with allied nations, on pain of contradiction with the very idea of ‘allied’ nation.
Appropriation

The final case for moral evaluation is that of appropriation, or in moral terms, theft. What justifies and what limits the acquisition of another nation or industry’s property in the world of espionage? We return again to our first principles to articulate both the justification and the limits. First, since nations have the right to employ means to defend themselves against enemy attack, it is permissible for them to try to determine how other nations may plan to attack them. Part of that determination involves understanding not only that another nation is developing a national security technology but what that technology involves. Discovering the full extent of a foreign technology often requires seeing it first hand, in other words, appropriating it. Hence, while it would be impermissible in the non-intelligence world to simply help oneself to technologies one finds interesting, intelligence officers are authorized by their nation’s self-defense rights to acquire through appropriation the hardware, blueprints, and property of other nations or industries serving them, if the failure to obtain that information threatens their national security.

That last conditional serves as the key limit on appropriation: only technologies or other properties that pertain to national security may be appropriated. Nations may not use their intelligence arms to conduct industrial espionage for the purposes of giving their own industries commercial advantages. Such conduct in peacetime is clearly theft and should be prohibited. Nations that violate this restriction in effect ‘nationalize’ their own industries, rendering them legitimate intelligence targets.

Conclusion

Acting morally does not necessarily mean states must give up obtaining critical information, but it does mean they may have to give up certain ways of obtaining it, even if that means intelligence officers must take greater risks. In practical terms this means intelligence professionals must take care in determining the nature as well as the targets of their operations. In terms of the nature of their operations, these are limited only by the collective self-defense conditions that make it possible and morally permissible to play the intelligence game in the first place. In terms of the targets of their operations, this means they may only target those who have voluntarily entered the game and avoid involving people who may be useful, but who have not, by any choice they have made, involved themselves. When it is necessary to involve innocents, they must observe the limitations imposed by the doctrine of double effect.

Because the work of the professional intelligence officer is indispensable to the national security duties of the state, espionage is itself a derivative moral obligation. This means we should dispense with the idea that somehow the work of the intelligence professional is not compatible with the dictates of morality. But since

---

* Wartime cases would obviously differ here, but it is not our intention in this essay to fully explicate the way in which wartime intelligence gathering limits differ from peacetime intelligence gathering limits.
the road to hell is paved with good intentions and lines do get crossed, it becomes imperative to establish moral boundaries, so intelligence professionals can execute their duties in clear conscience. This is not only good for the professional; it is good for the profession, and given the profession’s importance, to the nation as well.

Acknowledgements

We would like to thank Dr Beverly Milton Edwards of Queens University, Belfast, Northern Ireland, and Dr Sandra Visser, Valparaiso University, for their invaluable help in preparing and reviewing this paper. We are also grateful for the efforts of Major Todd Cyril, Foreign Area Officer, Captain Eric Larson, US Special Forces and Captain James Dickey, Military Intelligence Branch, who were instrumental in helping develop and articulate this argument.

References


Biographies

**Major Tony Pfaff**, is a Foreign Area Officer currently serving as a political-military analyst with the United States Joint Intelligence Directorate. A former Assistant Professor of Philosophy at West Point, he received a BA in Economics and Philosophy from Washington and Lee University and an MA in Philosophy from Stanford University (1997), where he was also a graduate fellow at the Stanford Center for Conflict and Negotiation. Major Pfaff has written and spoken on a variety of topics including military ethics, ethics of development, chaos theory, and conflict resolution.

**Dr. Jeffrey Tiel** is an associate professor of philosophy at Ashland University (Ashland, Ohio) where he also serves as the Director of the Academic Honors Program. He received his BA at the University of Scranton, his MA and PhD from Vanderbilt University (PhD 1996), and has been the recipient of the Salvatori Fellowship as well as numerous other awards and honors. He has published and presented numerous articles and papers related to military ethics themes including the ethics of biological warfare, the neutrality of states in an age of terror war, and journalism in psychological warfare.